

日 本 国 特 許 庁
JAPAN PATENT OFFICE

PCT/JP03/11706

12.09.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2002年 9月18日

出 願 番 号
Application Number: 特願2002-271473
[ST. 10/C]: [JP2002-271473]

出 願 人
Applicant(s): 三菱電機株式会社
理化学研究所

REC'D 30 OCT 2003

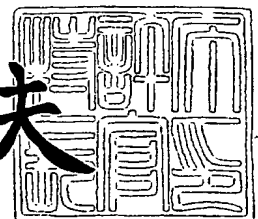
WIPO PCT

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2003年10月17日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 541636JP01

【提出日】 平成14年 9月18日

【あて先】 特許庁長官殿

【国際特許分類】 H03M 13/00
G09C 1/00 610

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 松本 渉

【発明者】

【住所又は居所】 埼玉県和光市広沢2番1号 理化学研究所内

【氏名】 渡辺 曜大

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【特許出願人】

【識別番号】 000006792

【氏名又は名称】 理化学研究所

【代理人】

【識別番号】 100089118

【弁理士】

【氏名又は名称】 酒井 宏明

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【物件名】 委任状 1

【援用の表示】 手続補足書にて提出の委任状

【包括委任状番号】 9803092

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 量子鍵配送方法および通信装置

【特許請求の範囲】

【請求項 1】 光子を量子通信路上に送信する第 1 の通信装置と当該光子を測定する第 2 の通信装置で構成された量子暗号システムにおける量子鍵配送方法において、

前記第 1 および第 2 の通信装置が、同一のパリティ検査行列 H ($n \times k$) を生成する検査行列生成ステップと、

前記第 1 の通信装置が、乱数列（送信データ）を発生し、さらに所定の送信コード（基底）をランダムに決定し、前記第 2 の通信装置が、所定の受信コード（基底）をランダムに決定する乱数発生ステップと、

前記第 1 の通信装置が、前記送信データと送信コードの組み合わせによって規定された量子状態で、光子を量子通信路上に送信する光子送信ステップと、

前記第 2 の通信装置が、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを得る光子受信ステップと、

前記第 1 および第 2 の通信装置が、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定された n ビットの受信データおよび対応する送信データを残し、その他を捨てるデータ削除ステップと、

前記第 1 の通信装置が、前記パリティ検査行列 H と n ビットの送信データに基づく k ビットの誤り訂正情報を、公開通信路を介して前記第 2 の通信装置に通知する誤り訂正情報通知ステップと、

前記第 2 の通信装置が、前記パリティ検査行列 H と n ビットの受信データと誤り訂正情報に基づいて、受信データの誤りを訂正する誤り訂正ステップと、

前記第 1 および第 2 の通信装置が、公開された誤り訂正情報に応じて誤り訂正後の共有情報（ n ）の一部（ k ）を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を装置間の共有鍵とする暗号鍵生成ステップと、

を含むことを特徴とする量子鍵配送方法。

【請求項 2】 前記検査行列生成ステップにあつては、基本行列として有限アフィン幾何を用い、ガウス近似法による最適化を行うこ

とによって、パリティ検査行列の最適な行と列の重み配分を探索する重み探索ステップと、

前記最適な重み配分に基づいて、前記有限アフィン幾何の行および列の重みを所定の手順でランダムに分割し、列と行の重みまたはどちらか一方が均一でない低密度パリティ検査符号のパリティ検査行列 H を生成する分割ステップと、

を含むことを特徴とする請求項 1 に記載の量子鍵配送方法。

【請求項 3】 前記検査行列生成ステップにあつては、さらに、「 $HG = 0$ 」を満たす生成行列 G ($(n-k) \times n$) から、 $G^{-1} \cdot G = I$ (単位行列) となる逆行列 G^{-1} ($n \times (n-k)$) を生成し、

前記暗号鍵生成ステップにあつては、逆行列 G^{-1} を用いて共有情報 (n) の一部 (k) を捨てることを特徴とする請求項 1 または 2 に記載の量子鍵配送方法。

【請求項 4】 前記検査行列生成ステップにあつては、さらに、 n 次元ベクトルを m ($m \leq n-k$) 次元ベクトルに写す写像 F で、任意の m 次元ベクトル v に対して、写像 F と「 $HG = 0$ 」を満たす生成行列 G の合成写像 $F \cdot G$ における逆像 $(F \cdot G)^{-1}(v)$ の元の個数が v によらず一定 (2^{n-k-m}) であるものを生成し、

前記暗号鍵生成ステップにあつては、写像 F を用いて共有情報 (n) の一部を捨てることを特徴とする請求項 1 または 2 に記載の量子鍵配送方法。

【請求項 5】 前記暗号鍵生成ステップにあつては、前記パリティ検査行列 H の列に対してランダム置換を実行し、前記パリティ検査行列 H の生成元の有限アフィン幾何 $AG(2, 2^s)$ の 1 列目の中から特定の「1」を選び、その位置を、公開通信路を介して交換し、前記置換後のパリティ検査行列から前記「1」に対応する分割後の位置 (列)、および巡回シフトされた各列における前記「1」に対応する分割後の位置 (列)、を特定し、その特定した位置 (列) に対応する共有情報 (n) の一部 (k) を捨てることを特徴とする請求項 2 に記載の量子鍵配送方法。

【請求項 6】 前記暗号鍵生成ステップにあつては、前記共有情報 (n) の一部 (k) を捨てた後、一方の装置が、正則なランダム行列 R ($(n-k) \times (n-k)$) を生成し、公開通信路を介して他方の通信装置に通知し、前記第 1 お

よび第2の通信装置が、それぞれ前記ランダム行列 R を暗号鍵に作用させることを特徴とする請求項3、4または5に記載の量子鍵配送方法。

【請求項7】 光子を量子通信路上に送信する通信装置において、

受信側の通信装置と同一のパリティ検査行列 H ($n \times k$) を生成する検査行列生成手段と、

乱数列(送信データ)を発生し、所定の送信コード(基底)をランダムに決定し、当該送信データと送信コードの組み合わせによって規定された量子状態で光子を量子通信路上に送信し、その後、前記受信側の通信装置における測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定された n ビットの送信データを残し、その他を捨てる送信手段と、

前記パリティ検査行列 H と n ビットの送信データに基づく k ビットの誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知する誤り訂正情報通知手段と、

公開した誤り訂正情報に応じて誤り訂正後の共有情報(n)の一部(k)を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を受信側の通信装置との共有鍵とする暗号鍵生成手段と、

を備えることを特徴とする通信装置。

【請求項8】 量子通信路上の光子を測定する通信装置において、

送信側の通信装置と同一のパリティ検査行列 H ($n \times k$) を生成する検査行列生成手段と、

所定の受信コード(基底)をランダムに決定し、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを再生し、その後、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定された n ビットの受信データを残し、その他を捨てる受信手段と、

公開通信路を介して受信した k ビットの誤り訂正情報と、前記パリティ検査行列 H と n ビットの受信データと、に基づいて、受信データの誤りを訂正する誤り訂正手段と、

公開された誤り訂正情報に応じて誤り訂正後の共有情報(n)の一部(k)を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を送信側の通信装置との共有

鍵とする暗号鍵生成手段と、

を備えることを特徴とする通信装置。

【請求項 9】 前記検査行列生成手段は、

基本行列として有限アフィン幾何を用い、ガウス近似法による最適化を行うことによって、パリティ検査行列の最適な行と列の重み配分を探索し、

前記最適な重み配分に基づいて、前記有限アフィン幾何の行および列の重みを所定の手順でランダムに分割し、

列と行の重みまたはどちらか一方が均一でない低密度パリティ検査符号のパリティ検査行列 H を生成することを特徴とする請求項 7 または 8 に記載の通信装置。

【請求項 10】 前記検査行列生成手段は、さらに、「 $HG=0$ 」を満たす生成行列 G ($(n-k) \times n$) から、 $G^{-1} \cdot G = I$ (単位行列) となる逆行列 G^{-1} ($n \times (n-k)$) を生成し、

前記暗号鍵生成手段は、逆行列 G^{-1} を用いて共有情報 (n) の一部 (k) を捨てることを特徴とする請求項 7、8 または 9 に記載の通信装置。

【請求項 11】 前記検査行列生成手段は、さらに、 n 次元ベクトルを m ($m \leq n-k$) 次元ベクトルに写す写像 F で、任意の m 次元ベクトル v に対して、写像 F と「 $HG=0$ 」を満たす生成行列 G の合成写像 $F \cdot G$ における逆像 $(F \cdot G)^{-1}(v)$ の元の個数が v によらず一定 (2^{n-k-m}) であるものを生成し、

前記暗号鍵生成手段は、写像 F を用いて共有情報 (n) の一部を捨てることを特徴とする請求項 7、8 または 9 に記載の通信装置。

【請求項 12】 前記暗号鍵生成手段にあつては、前記パリティ検査行列 H の列に対してランダム置換を実行し、前記パリティ検査行列 H の生成元の有限アフィン幾何 $AG(2, 2^s)$ の 1 列目の中から特定の「1」を選び、その位置を、公開通信路を介して交換し、前記置換後のパリティ検査行列から前記「1」に対応する分割後の位置 (列)、および巡回シフトされた各列における前記「1」に対応する分割後の位置 (列)、を特定し、その特定した位置 (列) に対応する共有情報 (n) の一部 (k) を捨てることを特徴とする請求項 9 に記載の通信装置。

【請求項 13】 前記暗号鍵生成手段は、前記共有情報 (n) の一部 (k) を捨てた後、正則なランダム行列 $R ((n-k) \times (n-k))$ を前記暗号鍵に作用させることを特徴とする請求項 10、11 または 12 に記載の通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法に関するものであり、特に、誤り訂正符号を用いてデータ誤りを訂正可能な量子鍵配送方法および当該量子鍵配送を実現可能な通信装置に関するものである。

【0002】

【従来の技術】

以下、従来の量子暗号システムについて説明する。近年、高速大容量な通信技術として光通信が広く利用されているが、このような光通信システムでは、光のオン/オフで通信が行われ、オンのときに大量の光子が送信されているため、量子効果が直接現れる通信系にはなっていない。

【0003】

一方、量子暗号システムでは、通信媒体として光子を用い、不確定性原理等の量子効果が生じるように 1 個の光子で 1 ビットの情報を伝送する。このとき、盗聴者が、その偏光、位相等の量子状態を知らずに適当に基底を選んで光子を測定すると、その量子状態に変化が生じる。したがって、受信側では、この光子の量子状態の変化を確認することによって、伝送データが盗聴されたかどうかを認識することができる。

【0004】

図 9 は、従来の偏光を利用した量子鍵配送の概要を示す図である。たとえば、水平垂直方向の偏光を識別可能な測定器では、量子通信路上の、水平方向 (0°) に偏光された光と垂直方向 (90°) に偏光された光とを正しく識別する。一方、斜め方向 (45° , 135°) の偏光を識別可能な測定器では、量子通信路上の、 45° 方向に偏光された光と 135° 方向に偏光された光とを正しくを識

別する。

【0005】

このように、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向 (0° , 90°) の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ 50% の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

【0006】

図9に示す従来の量子鍵配送では、上記不確定性 (ランダム性) を利用して、盗聴者に知られずに送信者と受信者との間で鍵を共有する (たとえば、非特許文献1参照。)。なお、送信者および受信者は、量子通信路以外に公開通信路を使用することができる。ここで、鍵の共有手順について説明する。

【0007】

まず、送信者は、乱数列 (1, 0 の列: 送信データ) を発生し、さらに送信コード (+: 水平垂直方向に偏光された光を識別可能な測定器に対応, \times : 斜め方向に偏光された光を識別可能な測定器に対応) をランダムに決定する。その乱数列と送信コードの組み合わせで、送信する光の偏光方向が自動的にきまる。ここでは、0 と + の組み合わせで水平方向に偏光された光を、1 と + の組み合わせで垂直方向に偏光された光を、0 と \times の組み合わせで 45° 方向に偏光された光を、1 と \times の組み合わせで 135° 方向に偏光された光を、量子通信路にそれぞれ送信する (送信信号)。

【0008】

つぎに、受信者は、受信コード (+: 水平垂直方向に偏光された光を識別可能な測定器, \times : 斜め方向に偏光された光を識別可能な測定器) をランダムに決定し、量子通信路上の光を測定する (受信信号)。そして、受信コードと受信信号の組み合わせによって受信データを得る。ここでは、受信データとして、水平方向に偏光された光と + の組み合わせで 0 を、垂直方向に偏光された光と + の組み合わせで 1 を、 45° 方向に偏光された光と \times の組み合わせで 0 を、 135° 方

向に偏光された光と×の組み合わせで0を、それぞれ得る。

【0009】

つぎに、受信者は、自身の測定が正しい測定器で行われたものかどうかを調べるために、受信コードを、公開通信路を介して送信者に対して送信する。受信コードを受け取った送信者は、正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信者に対して返信する。

【0010】

つぎに、受信者は、正しい測定器で受信した受信信号に対応する受信データだけを残し、その他を捨てる。この時点で、残された受信データは送信者と受信者との間で確実に共有できている。

【0011】

つぎに、送信者と受信者は、それぞれの通信相手に対して、共有データから選択した所定数のデータを、公開通信路を経由して送信する。そして、受け取ったデータが自信の持つデータと一致しているかどうかを確認する。たとえば、確認したデータの中に一致しないデータが1つでもあれば、盗聴者がいるものと判断して共有データを捨て、再度、鍵の共有手順を最初からやり直す。一方、確認したデータがすべて一致した場合には、盗聴者がいないと判断し、確認に使用したデータを捨て、残った共有データを送信者と受信者の共有鍵とする。

【0012】

また、上記従来の量子鍵配送方法の応用として、たとえば、伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法がある（たとえば、非特許文献2参照）。

【0013】

この方法では、送信者が、データ誤りを検出するために、送信データを複数のブロックに分割し、ブロック毎のパリティを公開通信路上に送信する。そして、受信者が、公開通信路を経由して受け取ったブロック毎のパリティと受信データにおける対応するブロックのパリティとを比較して、データ誤りをチェックする。このとき、異なるパリティがあった場合、受信者は、どのブロックのパリティが異なっているのかを示す情報を公開通信路上に返信する。そして、送信者は、

該当するブロックをさらに前半部のブロックと後半部のブロックに分割し、たとえば、前半部のパリティを公開通信路上に返信する（二分探索）。以降、送信者と受信者は、上記二分探索を繰り返し実行することによりエラービットの位置を特定し、最終的に受信者がそのビットを訂正する。

【0014】

さらに、送信者は、データに誤りがあるにもかかわらず、偶数個の誤りのために正しいと判定されたパリティがある場合を想定し、送信データをランダムに並べ替えて（ランダム置換）複数のブロックに分割し、再度、上記二分探索による誤り訂正処理を行う。そして、ランダム置換によるこの誤り訂正処理を繰り返し実行することによって、すべてのデータ誤りを訂正する。

【0015】

【非特許文献1】

Bennett, C. H. and Brassard, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing, In Proceedings of IEEE Conference on Computers, System and Signal Processing, Bangalore, India, pp.175-179 (DEC.1984).

【非特許文献2】

Brassard, G. and Salvail, L. 1993 Secret-Key Reconciliation by Public Discussion, In Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765, 410-423.

【0016】

【発明が解決しようとする課題】

しかしながら、上記図9に示す従来の量子鍵配送においては、誤り通信路を想定していないため、誤りがある場合には盗聴行為が存在したものとして上記共通データ（共通鍵）を捨てることとなり、伝送路によっては共通鍵の生成効率が非常に悪くなる、という問題があった。

【0017】

また、上記伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法においては、エラービットを特定するために膨大な回数のパリティのやりとりが発生し、さらに、ランダム置換による誤り訂正処理が所定回数にわたって行われるため、

誤り訂正処理に多大な時間を費やすことになる、という問題があった。

【0018】

本発明は、上記に鑑みてなされたものであって、極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法を得ることを目的とする。

【0019】

【課題を解決するための手段】

上述した課題を解決し、目的を達成するために、本発明にかかる量子鍵配送方法にあっては、光子を量子通信路上に送信する第1の通信装置と当該光子を測定する第2の通信装置で構成された量子暗号システムにて実行され、たとえば、前記第1および第2の通信装置が、同一のパリティ検査行列 H ($n \times k$) を生成する検査行列生成ステップと、前記第1の通信装置が、乱数列（送信データ）を発生し、さらに所定の送信コード（基底）をランダムに決定し、前記第2の通信装置が、所定の受信コード（基底）をランダムに決定する乱数発生ステップと、前記第1の通信装置が、前記送信データと送信コードの組み合わせによって規定された量子状態で、光子を量子通信路上に送信する光子送信ステップと、前記第2の通信装置が、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを得る光子受信ステップと、前記第1および第2の通信装置が、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定された n ビットの受信データおよび対応する送信データを残し、その他を捨てるデータ削除ステップと、前記第1の通信装置が、前記パリティ検査行列 H と n ビットの送信データに基づく k ビットの誤り訂正情報を、公開通信路を介して前記第2の通信装置に通知する誤り訂正情報通知ステップと、前記第2の通信装置が、前記パリティ検査行列 H と n ビットの受信データと誤り訂正情報に基づいて、受信データの誤りを訂正する誤り訂正ステップと、前記第1および第2の通信装置が、公開された誤り訂正情報に応じて誤り訂正後の共有情報 (n) の一部 (k) を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を装置間の共有鍵とする暗号鍵生成ステップと、を含むことを特徴とする。

【0020】

この発明によれば、確定的で特性が安定した「Irregular-LDPC 符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、さらに、公開された誤り訂正情報に応じて共有情報の一部を捨てる。

【0021】

【発明の実施の形態】

以下に、本発明にかかる量子鍵配送方法の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。また、以下では、例として偏光を利用する量子鍵配送について説明するが、本発明は、たとえば、位相を利用するもの、周波数を利用するもの等にも適用可能であり、どのような量子状態を利用するかについては特に限定しない。

【0022】

実施の形態 1.

量子鍵配送は、盗聴者の計算能力によらず、安全性の保証された鍵配送方式であるが、たとえば、より効率よく共有鍵を生成するためには、伝送路を通ることによって発生するデータの誤りを取り除く必要がある。そこで、本実施の形態では、極めて高い特性をもつことが知られている低密度パリティ検査 (LDPC: Low-Density Parity-Check) 符号を用いて誤り訂正を行う量子鍵配送について説明する。

【0023】

図 1 は、本発明にかかる量子暗号システムにおける通信装置 (送信機, 受信機) の構成を示す図である。この量子暗号システムは、情報 m_A を送信する機能を備えた送信側の通信装置と、伝送路上で雑音等の影響を受けた情報 m_A 、すなわち情報 m_B を受信する機能を備えた受信側の通信装置と、から構成される。

【0024】

また、送信側の通信装置は、量子通信路を介して情報 m_A を送信し、公開通信路を介してシンδροーム s_A を送信し、これらの送信情報に基づいて暗号鍵 (受信側との共通鍵) を生成する暗号鍵生成部 1 と、暗号化部 2 1 が暗号鍵に基づいて暗号化したデータを、送受信部 2 2 が公開通信路を介してやりとりする通信部 2 と、を備え、受信側の通信装置は、量子通信路を介して情報 m_B を受信し、公

開通信路を介してシンドローム s_A を受信し、これらの受信情報に基づいて暗号鍵（送信側との共通鍵）を生成する暗号鍵生成部 3 と、暗号化部 4 2 が暗号鍵に基づいて暗号化したデータを、送受信部 4 1 が公開通信路を介してやりとりする通信部 4 と、を備える。

【0025】

上記送信側の通信装置では、量子通信路上に送信する情報 m_A として、偏光フィルターを用いて所定の方向に偏光させた光（図 9 参照）を、受信側の通信装置に対して送信する。一方、受信側の通信装置では、水平垂直方向（ 0° ， 90° ）の偏光を識別可能な測定器と斜め方向（ 45° ， 135° ）の偏光を識別可能な測定器とを用いて、量子通信路上の、水平方向（ 0° ）に偏光された光と垂直方向（ 90° ）に偏光された光と 45° 方向に偏光された光と 135° 方向に偏光された光とを識別する。なお、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（ 0° ， 90° ）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ 50% の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

【0026】

以下、上記量子暗号システムにおける各通信装置の動作、すなわち、本実施の形態における量子鍵配送について詳細に説明する。図 2 は、本実施の形態の量子鍵配送を示すフローチャートであり、詳細には、（a）は送信側の通信装置の処理を示し、（b）は受信側の通信装置の処理を示す。

【0027】

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部 10，30 が、特定の線形符号のパリティ検査行列 H （ $n \times k$ ）を求め、このパリティ検査行列 H から「 $HG = 0$ 」を満たす生成行列 G （ $(n-k) \times n$ ）を求め、さらに、 $G^{-1} \cdot G = I$ （単位行列）となる G の逆行列 G^{-1} （ $n \times (n-k)$ ）を求める（ステップ S1，ステップ S11）。本実施の形態では、上記特定の線形符号として、シャノン限界に極めて近い優れた特性をもつ LDPC 符

号を用いた場合の量子鍵配送について説明する。なお、本実施の形態では、誤り訂正方式としてLDPC符号を用いることとしたが、これに限らず、たとえば、ターボ符号等の他の線形符号を用いることとしてもよい。また、たとえば、後述する誤り訂正情報（シンドローム）が適当な行列 H と情報 m_A の積 Hm_A で表される誤り訂正プロトコル（たとえば、従来技術にて説明した「伝送路上におけるデータ誤りを訂正可能な量子鍵配送」に相当する誤り訂正プロトコル）であれば、すなわち、誤り訂正情報と情報 m_A の線形性が確保されるのであれば、その行列 H を用いることとしてもよい。

【0028】

ここで、上記パリティ検査行列生成部10におけるLDPC符号の構成法について、詳細には、有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法（図2ステップS1の詳細）について説明する。図3は、有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法を示すフローチャートである。なお、パリティ検査行列生成部30については、パリティ検査行列生成部10と同様に動作するのでその説明を省略する。また、本実施の形態における検査行列生成処理は、たとえば、設定されるパラメータに応じてパリティ検査行列生成部10で実行する構成としてもよいし、通信装置外部の他の制御装置（計算機等）で実行することとしてもよい。本実施の形態における検査行列生成処理が通信装置外部で実行される場合は、生成済みの検査行列が通信装置に格納される。以降の実施の形態では、パリティ検査行列生成部10で上記処理を実行する場合について説明する。

【0029】

まず、パリティ検査行列生成部10では、「Irregular-LDPC符号」用の検査行列のベースとなる有限アフィン幾何符号 $AG(2, 2^s)$ を選択する（図3、ステップS21）。ここでは、行の重みと列の重みがそれぞれ 2^s となる。図4は、たとえば、有限アフィン幾何符号 $AG(2, 2^2)$ のマトリクスを示す図（空白は0を表す）である。

【0030】

つぎに、パリティ検査行列生成部10では、列の重みの最大値 r_1 （ $2 < r_1 \leq$

2s) を決定する (ステップ S 2 2)。そして、符号化率 $rate$ (1-シンドローム長/鍵の長さ) を決定する (ステップ S 2 2)。

【0031】

つぎに、パリティ検査行列生成部 10 では、ガウス近似法 (Gaussian Approximation) による最適化を用いて、暫定的に、列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_μ を求める (ステップ S 2 3)。なお、行の重み配分の生成関数 $\rho(x)$ は $\rho(x) = \rho_\mu x^{\mu-1} + (1-\rho_\mu) x^\mu$ とする。また、重み μ は $\mu \geq 2$ の整数であり、 ρ_μ は行における重み μ の割合を表す。

【0032】

つぎに、パリティ検査行列生成部 10 では、有限アフィン幾何の行の分割により構成可能な、行の重み $\{\mu, \mu+1\}$ を選択し、さらに (1) 式を満たす分割係数 $\{b_\mu, b_{\mu+1}\}$ を求める (ステップ S 2 4)。なお、 $b_\mu, b_{\mu+1}$ は非負の整数とする。

$$b_\mu + b_{\mu+1}(\mu+1) = 2s \quad \dots (1)$$

【0033】

具体的には、下記 (2) 式から b_μ を求め、上記 (1) 式から $b_{\mu+1}$ を求める。

【0034】

【数 1】

$$\arg \min_{b_\mu} \left| \varphi_\mu - \frac{\mu \times b_\mu}{2^s} \right| \quad \dots (2)$$

【0035】

つぎに、パリティ検査行列生成部 10 では、上記決定したパラメータ $\mu, \mu+1, b_\mu, b_{\mu+1}$ によって (上記行の分割処理によって) 更新された行の重みの比率 $\rho'_\mu, \rho'_{\mu+1}$ を (3) 式により求める (ステップ S 2 5)。

【0036】

【数2】

$$\begin{aligned}\varphi'_\mu &= \frac{\mu \times b_\mu}{2^s} \\ \varphi'_{\mu+1} &= \frac{(\mu+1) \times b_{\mu+1}}{2^s}\end{aligned} \quad \dots \quad (3)$$

【0037】

つぎに、パリティ検査行列生成部10では、ガウス近似法による最適化を用いて、さらに上記で求めた μ , $\mu+1$, $\rho\mu'$, $\rho\mu+1'$ を固定のパラメータとして、暫定的に、列の重み配分 $\lambda(\gamma_i)$ を求める(ステップS26)。なお、重み γ_i は $\gamma_i \geq 2$ の整数であり、 $\lambda(\gamma_i)$ は列における重み γ_i の割合を表す。また、列数が1以下となる重み($\lambda(\gamma_i) \leq \gamma_i/w_t$, i は正の整数)を候補から削除する。ただし、 w_t は $AG(2, 2^s)$ に含まれる1の総数を表す。

【0038】

つぎに、上記で求めた重み配分を満たし、かつ下記(4)式を満たす、列の重み候補のセット $\{\gamma_1, \gamma_2, \dots, \gamma_l \mid \gamma_l \leq 2^s\}$ を選択する(ステップS27)。そして、下記の(4)式を満たさない列の重み γ_i が存在する場合には、その列の重みを候補から削除する。

【0039】

【数3】

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,\ell} \\ a_{2,1} & a_{2,2} & \dots & a_{2,\ell} \\ \vdots & & \dots & \vdots \end{bmatrix} \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_\ell \end{bmatrix} = \begin{bmatrix} 2^s \\ 2^s \\ \vdots \\ 2^s \end{bmatrix} \quad \dots \quad (4)$$

【0040】

なお、各 a は、列の重み 2^s を構成するための $\{\gamma_1, \gamma_2, \dots, \gamma_l\}$ に対する非負の整数となる係数を表し、 i, j は正の整数であり、 γ_i は列の重みを表し、 γ_l は列の最大重みを表す。

【0041】

つぎに、パリティ検査行列生成部10では、ガウス近似法による最適化を用いて、さらに上記で求めた μ , $\mu+1$, $\rho\mu'$, $\rho\mu+1'$ と $\{\gamma_1, \gamma_2, \dots, \gamma_l\}$ を固定パラメータとして、列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 $\rho\mu$ を求める(ステップS28)。

【0042】

つぎに、パリティ検査行列生成部10では、分割処理を行う前に、列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 $\rho\mu$ を調整する(ステップS29)。なお、調整後の各重みの配分は、可能な限りガウス近似法で求めた値に近い値にする。図5は、ステップS29における最終的な列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 $\rho\mu$ を示す図である。

【0043】

最後に、パリティ検査行列生成部10では、有限アフィン幾何における行および列を分割して(ステップS30)、 $n \times k$ のパリティ検査行列Hを生成する。本発明における有限アフィン幾何符号の分割処理は、規則的に分割するのではなく、各行または各列から「1」の番号をランダムに抽出する(後述するランダム分割の具体例を参照)。なお、この抽出処理は、ランダム性が保持されるのであればどのような方法を用いてもよい。

【0044】

具体的にいうと、EG(2, 2⁵)における1列中の「1」の行番号が、
 $B_1(x) = \{1, 32, 114, 136, 149, 223, 260, 382, 402, 438, 467, 507, 574, 579, 588, 622, 634, 637, 638, 676, 717, 728, 790, 851, 861, 879, 947, 954, 971, 977, 979, 998\}$
 の場合、分割後の行列における1～4列目 $R_m(n)$ は、 $B_1(x)$ から「1」の番号がランダムに抽出され、たとえば、
 $R_1(n) = \{1, 114, 574, 637, 851, 879, 977, 979\}$
 $R_2(n) = \{32, 136, 402, 467, 588, 728, 861, 971\}$
 $R_3(n) = \{149, 260, 382, 438, 579, 638, 717, 998\}$
 $R_4(n) = \{223, 507, 622, 634, 676, 790, 947, 954\}$
 となる。

【0045】

ここで、上記ランダム分割の一例、すなわち、上記「乱数系列のラテン方陣を用いた分割方法」を詳細に説明する。ここでは、ランダム分割を行う場合のランダム系列を容易かつ確定的に生成する。この方法による利点は、送信側と受信側が同じランダム系列を生成できることにある。

【0046】

(1) 基本のランダム系列を作成する。ここでは、有限アフィン幾何 $AG(2, 2^s)$ を用い、 P を $P \geq 2^s$ を満たす最小の素数とした場合の、基本のランダム系列 $C(i)$ を (5) 式にしたがって作成する。

$$C(1) = 1$$

$$C(i+1) = G_0 \times C(i) \mod P \quad \dots (5)$$

なお、 $i = 0, 1, \dots, P-2$ とし、 G_0 はガロア体 $GF(P)$ の原始元である。また、系列長が 2^s となるように、 2^s より大きい数を $C(i)$ の中から削除し、削除後の $C(i)$ を基本のランダム系列とする。

【0047】

(2) 基本のランダム系列 $C(i)$ を一定間隔で読み出すためにスキップ間隔 $S(j)$ を以下の (6) 式のように定義する。

$$S(j) = j \quad j = 1, 2, \dots, 2^s \quad \dots (6)$$

【0048】

(3) 以下の (7) 式で置換パターン $LB_j(i)$ を作成する。

$$LB_j(i) = (S(j) \times i) \mod P + 1$$

$$j = 1, 2, \dots, 2^s$$

$$i = 1, 2, \dots, P-1 \quad \dots (7)$$

なお、 $LB_j(i)$ も 2^s より大きい数字は削除する。

【0049】

(4) q 列 i 行で j 番目のラテン方陣行列 $L_{jq}(i)$ を以下の (8) 式で算出する。

$$L_{jq}(i) = LB_j((q+i-2) \mod 2^s + 1)$$

$$j = 1, 2, \dots, 2^s$$

$$i = 1, 2, \dots, 2^s$$

$$q = 1, 2, \dots, 2^s \quad \dots (8)$$

【0050】

(5) ラテン方阵行列 $L_{jq}(i)$ にしたがって列と行を分割する。列の分割では、 g_0, g_0, \dots, g_{n-1} をパリティ検査行列 H の列ベクトルとし、 $g_c'(k)$ を $g_c, c = 0, 1, \dots, n-1$ の列の中の k 番目の「1」とする。また、 g_c 中の「1」の位置の集合を G_c とする ((9) 式参照)。

$$G_c = \{g_c'(k), k = 1, 2, \dots, 2^s\} \quad \dots (9)$$

たとえば、 $AG(2, 2^3)$ の $c = 1$ 番目の列の「1」の行番号は、 $G_1 = \{1, 3, 8, 20, 23, 24, 34, 58\}$ となる。そして、この c 列目の列ベクトルを $g_c'(k)$ で表現すると、(10) 式のように表すことができる。

$$g_c'(1) = ((c-1) + 1) \bmod (2^{2s}-1)$$

$$g_c'(2) = (g_c'(1) + 2) \bmod (2^{2s}-1)$$

$$g_c'(3) = (g_c'(2) + 5) \bmod (2^{2s}-1)$$

$$g_c'(4) = (g_c'(3) + 12) \bmod (2^{2s}-1)$$

$$g_c'(5) = (g_c'(4) + 3) \bmod (2^{2s}-1)$$

$$g_c'(6) = (g_c'(5) + 1) \bmod (2^{2s}-1)$$

$$g_c'(7) = (g_c'(6) + 10) \bmod (2^{2s}-1)$$

$$g_c'(8) = (g_c'(7) + 24) \bmod (2^{2s}-1) \quad \dots (10)$$

【0051】

ここで、パリティ検査行列 H の各列 g_c を、上記 (4) 式を満たす列の次数と係数に基づいて、新しい列 $g_{c,e}$ に分割する。そして、 $g_{c,e}'(r)$ を新しい列 $g_{c,e}$ 中の r 行目の「1」とする。また、 $g_{c,e}$ 中の「1」の位置の集合を $G_{c,e}$ とする ((11) 式参照)。

$$G_{c,e} = \{g_{c,e}'(r), r = 1, 2, \dots\} \quad \dots (11)$$

【0052】

そして、ラテン方阵行列群を用いて、下記 (12) 式にしたがって分割するエッジの選択を行う。なお、 $a_{t,1}, a_{t,2}, \dots, a_{t,l}$ と $\gamma_1, \gamma_2, \dots, \gamma_l$ は、上記式 (4) を満たす係数と次数である。また、 t は (4) 式の係数行列の行番号を

示している。また、 t 行目の式で分割する有限アフィン平面の列数を n_t とし、係数行列の行番号の最大値を t_m とすると、 t は (13) 式で表すことができる。

【0053】

【数4】

$$\begin{aligned} g'_{c,e}(r) &= g'_c(L_{j,q}(i)) \\ j &= c/2^s \\ q &= ((c-1) \bmod 2^s) + 1 \\ i &= r + \sum_{m=1}^{\ell} \min(a_{t,m}, \max(0, e-1 - \sum_{n=1}^{m-1} a_{t,n})) \cdot \gamma_m \end{aligned} \quad \dots (12)$$

【0054】

【数5】

$$t \begin{cases} 1(1 \leq c \leq n_1) \\ 2(n_1 + 1 \leq c \leq n_1 + n_2) \\ \vdots \\ t_m(\sum_{i=1}^{t_m-1} n_i + 1 \leq c \leq \sum_{i=2}^{t_m} n_i) \end{cases} \quad \dots (13)$$

【0055】

つぎに、上記 (1) ~ (4) の分割処理を、具体例を挙げて説明する。例として、 $AG(2, 2^3)$ の $c = 16$ 番目の列の「1」の行番号を $G_{16} = \{10, 16, 18, 23, 35, 38, 39, 49\}$ と定義する。図6は、ランダム系列のラテン方陣行列による分割手順を示す図である。図示のラテン方陣行列 $L_{j,q}(i)$ の結果を用いて手順 (5) を実行すると、新しい列 $g_{16,e}$ 中の「1」は (14) 式のように表すことができる。

$$\begin{aligned} g_{16,1}'(1) &= g_{16}'(L_{2,8}(1)) = g_{16}'(3) = 18 \\ g_{16,1}'(2) &= g_{16}'(L_{2,8}(2)) = g_{16}'(2) = 16 \end{aligned}$$

$$\begin{aligned}
g_{16,2'}(1) &= g_{16'}(L_{2,8}(3)) = g_{16'}(8) = 49 \\
g_{16,2'}(2) &= g_{16'}(L_{2,8}(4)) = g_{16'}(7) = 39 \\
g_{16,3'}(1) &= g_{16'}(L_{2,8}(5)) = g_{16'}(6) = 38 \\
g_{16,3'}(2) &= g_{16'}(L_{2,8}(6)) = g_{16'}(1) = 10 \\
g_{16,4'}(1) &= g_{16'}(L_{2,8}(7)) = g_{16'}(4) = 23 \\
g_{16,4'}(2) &= g_{16'}(L_{2,8}(8)) = g_{16'}(5) = 35 \quad \dots (14)
\end{aligned}$$

【0056】

その結果、16番目の列は以下のように分割される。

$$G_{16,1} = \{18 \ 16\}$$

$$G_{16,2} = \{49 \ 39\}$$

$$G_{16,3} = \{38 \ 10\}$$

$$G_{16,4} = \{23 \ 35\}$$

【0057】

このように、本実施の形態では、上記有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法（図2、ステップS1）を実行することによって、確定的で特性が安定した「Irregular-LDPC符号」用の検査行列 $H (n \times k)$ を生成することができる。

【0058】

上記のように、パリティ検査行列 H 、生成行列 G 、 G^{-1} ($G^{-1} \cdot G = I$: 単位行列) を生成後、つぎに、送信側の通信装置では、乱数発生部11が、乱数列 (1, 0の列: 送信データ) を発生し、さらに送信コード (+: 水平垂直方向に偏光された光を識別可能な測定器に対応したコード, \times : 斜め方向に偏光された光を識別可能な測定器に対応したコード) をランダムに決定する (ステップS2)。一方、受信側の装置では、乱数発生部31が、受信コード (+: 水平垂直方向に偏光された光を識別可能な測定器に対応したコード, \times : 斜め方向に偏光された光を識別可能な測定器に対応したコード) をランダムに決定する (ステップS12)。

【0059】

つぎに、送信側の通信装置では、光子生成部12が、上記乱数列と送信コード

の組み合わせで自動的に決まる偏光方向で光子を送信する（ステップS3）。たとえば、0と+の組み合わせで水平方向に偏光された光を、1と+の組み合わせで垂直方向に偏光された光を、0と×の組み合わせで45°方向に偏光された光を、1と×の組み合わせで135°方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

【0060】

光子生成部12の光信号を受け取った受信側の通信装置の光子受信部32では、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって自動的に決まる受信データを得る（ステップS13）。ここでは、受信データとして、水平方向に偏光された光と+の組み合わせで0を、垂直方向に偏光された光と+の組み合わせで1を、45°方向に偏光された光と×の組み合わせで0を、135°方向に偏光された光と×の組み合わせで0を、それぞれ得る。

【0061】

つぎに、受信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べるために、乱数発生部31が、受信コードを、公開通信路を介して送信側の通信装置に対して送信する（ステップS13）。受信コードを受け取った送信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信側の通信装置に対して送信する（ステップS3）。そして、受信側の通信装置および送信側の通信装置では、正しい測定器で受信した受信信号に対応するデータだけを残し、その他を捨てる（ステップS3, S13）。その後、残ったデータをメモリ等に保存し、その先頭から順にnビットを読み出し、送信データ m_A と受信データ m_B （ m_B は伝送路上で雑音等の影響を受けた m_A ）を生成する。すなわち、ここでは、共有鍵生成処理が終わる度につぎのnビットを読み出し、その都度、送信データ m_A と受信データ m_B を生成する。本実施の形態では、正しい測定器で受信した受信信号に対応するビットの位置が、送信側の通信装置と受信側の通信装置との間で共有できている。

【0062】

つぎに、送信側の通信装置では、シンドローム生成部14が、パリティ検査行

列 H ($n \times k$) と送信データ m_A を用いて m_A のシンドローム $S_A = H m_A$ を計算し、その結果を、公開通信路通信部 13, 公開通信路を介して受信側の通信装置に通知する (ステップ S4)。この段階で、 m_A のシンドローム S_A (k ビット分の情報) は盗聴者に知られる可能性がある。一方、受信側の通信装置では、公開通信路通信部 34 にて m_A のシンドローム S_A を受信し、それをシンドローム復号部 33 に通知する (ステップ S14)。

【0063】

シンドローム復号部 33 では、パリティ検査行列 H と受信データ m_B を用いて m_B のシンドローム $S_B = H m_B$ を計算し、さらに、 m_A のシンドローム S_A と m_B のシンドローム S_B を用いてシンドローム $S = S_A + S_B$ を計算する (ステップ S15)。そして、シンドローム S に基づいて送信データ m_A を推定する (ステップ S16)。ここでは、 $m_A = m_B + e$ (雑音等) と仮定し、式 (15) に示すようにシンドローム S を変形した後、シンドローム復号により e を求め、送信データ m_A を求める (ステップ S16)。なお、 $S_A + S_B$, $m_A + e$ の $+$ は排他的論理和を表す。

$$\begin{aligned} S &= S_A + S_B \\ &= H m_A + H m_B \\ &= H (m_A + m_B) \\ &= H (m_B + e + m_B) \\ &= H e \end{aligned} \quad \dots (15)$$

【0064】

最後に、受信側の通信装置では、共有鍵生成部 35 が、公開された誤り訂正情報 (盗聴された可能性のある上記 k ビット分の情報: S_A) に応じて共有情報 (m_A) の一部を捨てて、 $n - k$ ビット分の情報量を備えた暗号鍵 r を生成する (ステップ S17)。すなわち、共有鍵生成部 35 では、先に計算しておいた G^{-1} ($n \times (n - k)$) を用いて下記 (16) 式により暗号鍵 r を生成する。受信側の通信装置は、この暗号鍵 r を送信側の通信装置との共有鍵とする。

$$r = G^{-1} m_A \quad \dots (16)$$

【0065】

一方、送信側の通信装置においても、共有鍵生成部 15 が、公開された誤り訂正情報（盗聴された可能性のある上記 k ビット分の情報： S_A ）に応じて共有情報（ m_A ）の一部を捨てて、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する（ステップ S5）。すなわち、共有鍵生成部 15 では、先に計算しておいた $G^{-1} (n \times (n-k))$ を用いて上記（16）式により暗号鍵 r を生成する（ステップ S5）。送信側の通信装置は、この暗号鍵 r を受信側の通信装置との共有鍵とする。

【0066】

このように、本実施の形態においては、確定的で特性が安定した「Irregular-LDPC 符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てる構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。

【0067】

なお、本実施の形態では、 $HG=0$ を満たす生成行列 $G ((n-k) \times n)$ から、 $G^{-1} \cdot G = I$ （単位行列）となる逆行列 $G^{-1} (n \times (n-k))$ を生成し、当該逆行列 G^{-1} を用いて共有情報（ n ）の一部（ k ）を捨てて、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成することとしたが、これに限らず、共有情報（ n ）の一部を捨てて、 $m (m \leq n-k)$ ビット分の情報量を備えた暗号鍵 r を生成することとしてもよい。具体的にいうと、 n 次元ベクトルを m 次元ベクトルに写す写像 $F(\cdot)$ を想定する。 $F(\cdot)$ は、共有鍵の安全性を保証するために、「任意の m 次元ベクトル v に対して、写像 F と生成行列 G の合成写像 $F \cdot G$ における逆像 $(F \cdot G)^{-1}(v)$ の元の個数が v によらず一定 (2^{n-k-m}) である」、という条件を満たす必要がある。このとき、共有鍵 r は、 $r = F(m_A)$ となる。

【0068】

実施の形態 2.

実施の形態 2 では、前述した実施の形態 1 における暗号鍵の秘匿性をさらに増強させる。

【0069】

図 7 は、本発明にかかる量子暗号システムの実施の形態 2 の構成を示す図である。なお、先に説明した実施の形態 1 と同様の構成については、同一の符号を付してその説明を省略する。量子通信路で盗聴された情報に対して秘匿性を増強させるためには、盗聴されたビット数分をハッシュ関数により圧縮する必要がある。しかしながら、ハッシュ関数は、その特性により盗聴されやすい位置が存在する。そこで、本実施の形態においては、その位置をランダムに並べ替えることによって対応する。

【0070】

図 8 は、実施の形態 2 の量子鍵配送を示すフローチャートであり、詳細には、送信側の通信装置の処理を示す。送信側の通信装置のランダム置換部 16 では、正則なランダム行列 R ($(n-k) \times (n-k)$) を生成し、当該 R を共有鍵生成部 15 に通知し、さらに、当該 R を、公開通信路を介して受信側の通信装置の共有鍵生成部 35 に通知する（ステップ S6）。なお、図 7 および図 8 では、一例として、送信側の通信装置でランダム行列 R を生成／送信しているが、これに限らず、この処理は、受信側の通信装置で行うこととしてもよい。

【0071】

その後、送信側の通信装置では、共有鍵生成部 15 が、公開された誤り訂正情報（盗聴された可能性のある上記 k ビット分の情報： S_A ）に応じて共有情報（ m_A ）の一部を捨てて、さらに、受け取ったランダム行列 R を用いて秘匿性を増強して、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する（ステップ S5）。すなわち、共有鍵生成部 15 では、先に計算しておいた G^{-1} ($n \times (n-k)$) と受け取ったランダム行列 R ($(n-k) \times (n-k)$) を用いて下記（17）式により暗号鍵 r を生成する。送信側の通信装置は、この暗号鍵 r を受信側の通信装置との共有鍵とする。

$$r = R G^{-1} m_A \quad \dots (17)$$

【0072】

一方、受信側の通信装置においても、共有鍵生成部 35 が、公開された誤り訂正情報（盗聴された可能性のある上記 k ビット分の情報： S_A ）に応じて共有情報（ m_A ）の一部を捨てて、さらに、受け取ったランダム行列 R を用いて秘匿性を増強して、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する（ステップ S17）。すなわち、共有鍵生成部 15 では、先に計算しておいた G^{-1} （ $n \times (n-k)$ ）と受け取ったランダム行列 R （ $(n-k) \times (n-k)$ ）を用いて上記（17）式により暗号鍵 r を生成する（ステップ S17）。受信側の通信装置は、この暗号鍵 r を送信側の通信装置との共有鍵とする。

【0073】

このように、本実施の形態においては、確定的で特性が安定した「Irregular-LDPC 符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てて、さらに正則なランダム行列を用いて共有情報を並べ替える構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。さらに、正則なランダム行列を用いて共有情報を並べ替えることとしたため、秘匿性を増強させることができる。

【0074】

なお、本実施の形態においても、実施の形態 1 と同様に、共有情報（ n ）の一部を捨てて、 m （ $m \leq n-k$ ）ビット分の情報量を備えた暗号鍵 r を生成することとしてもよい。この場合、共有鍵 r は、 $r = RF(m_A)$ となる。

【0075】

実施の形態 3.

先に説明した実施の形態 1 では、生成行列 G^{-1} を用いて共有情報の一部を捨てていた。これに対して、実施の形態 3 では、生成行列 G^{-1} を用いずに、パリティ検査行列 H の特性を用いて共有情報の一部を捨てる。なお、本実施の形態の構成

は、先に説明した実施の形態 1 の図 1 と同様である。

【0076】

以下、実施の形態 3 の量子鍵配送について説明する。ここでは、先に説明した図 2 と異なる処理についてのみ説明する。

【0077】

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部 10、30 が、特定の線形符号のパリティ検査行列 H ($n \times k$) を求める (ステップ S1, ステップ S11)。なお、有限アフィン幾何に基づく「Irregular-LDPC 符号」の構成法 (図 2 ステップ S1 の詳細) については、先に説明した実施の形態 1 の図 3 と同様である。

【0078】

そして、実施の形態 1 と同様の手順でステップ S2 ~ S4 を実行後、受信側の通信装置では、共有鍵生成部 35 が、公開された誤り訂正情報 (盗聴された可能性のある上記 k ビット分の情報: S_A) に応じて共有情報 (m_A) の一部を捨てて、 $n - k$ ビット分の情報量を備えた暗号鍵 r を生成する (ステップ S17)。具体的には、共有鍵生成部 35 が、上記ステップ S11 で生成したパリティ検査行列の列に対してランダム置換を行う。そして、送信側の通信装置との間で捨てるビットに関する情報を、公開通信路を介して交換する。ここでは、元の有限アフィン幾何 $AG(2, 2^s)$ の 1 列目の中から特定の「1」を選び、その位置を、公開通信路を介して交換する。

【0079】

その後、共有鍵生成部 35 では、上記置換後のパリティ検査行列から上記「1」に対応する分割後の位置、および巡回シフトされた各列における上記「1」に対応する分割後の位置を特定し、その特定した位置に対応する共有情報 m_A 内のビットを捨てて、残りのデータを暗号鍵 r とする。受信側の通信装置は、この暗号鍵 r を送信側の通信装置との共有鍵とする。

【0080】

一方、送信側の通信装置においても、共有鍵生成部 15 が、公開された誤り訂正情報 (盗聴された可能性のある上記 k ビット分の情報: S_A) に応じて共有情

報 (m_A) の一部を捨てて、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する (ステップ S5)。具体的には、共有鍵生成部 15 が、上記ステップ S1 で生成したパリティ検査行列の列に対して上記と同様のランダム置換を行う。そして、上記捨てるビットに関する情報を、公開通信路を介して交換する。

【0081】

その後、共有鍵生成部 15 では、上記置換後のパリティ検査行列から上記「1」に対応する分割後の位置、および巡回シフトされた各列における上記「1」に対応する分割後の位置を特定し、その特定した位置に対応する共有情報 m_A 内のビットを捨てて、残りのデータを暗号鍵 r とする。送信側の通信装置は、この暗号鍵 r を受信側の通信装置との共有鍵とする。

【0082】

このように、本実施の形態においては、生成行列 G^{-1} を用いずに、パリティ検査行列 H の特性を用いて共有情報の一部を捨てる構成とした。これにより、実施の形態 1 と同様の効果が得られるとともに、さらに、複雑な生成行列 G 、 G^{-1} の演算処理を削除することができる。

【0083】

なお、本実施の形態においては、パリティ検査行列 H の特性を用いて共有情報の一部を捨てて、さらに、実施の形態 2 と同様に、正則なランダム行列を用いて共有情報を並べ替える構成としてもよい。これにより、秘匿性を増強させることができる。

【0084】

【発明の効果】

以上、説明したとおり、本発明によれば、確定的で特性が安定した「Irregular-LDPC符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる、という効果を奏する。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保

証された共通鍵を生成することができる、という効果を奏する。

【図面の簡単な説明】

【図 1】 本発明にかかる量子暗号システムの実施の形態 1 の構成を示す図である。

【図 2】 実施の形態 2 の量子鍵配送を示すフローチャートである。

【図 3】 有限アフィン幾何に基づく「Irregular-LDPC 符号」の構成法を示すフローチャートである。

【図 4】 有限アフィン幾何符号 $AG(2, 2^2)$ のマトリクスを示す図である。

【図 5】 最終的な列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_μ を示す図である。

【図 6】 ランダム系列のラテン方陣行列による分割手順を示す図である。

【図 7】 本発明にかかる量子暗号システムの実施の形態 2 の構成を示す図である。

【図 8】 実施の形態 2 の量子鍵配送を示すフローチャートである。

【図 9】 従来の量子鍵配送の概要を示す図である。

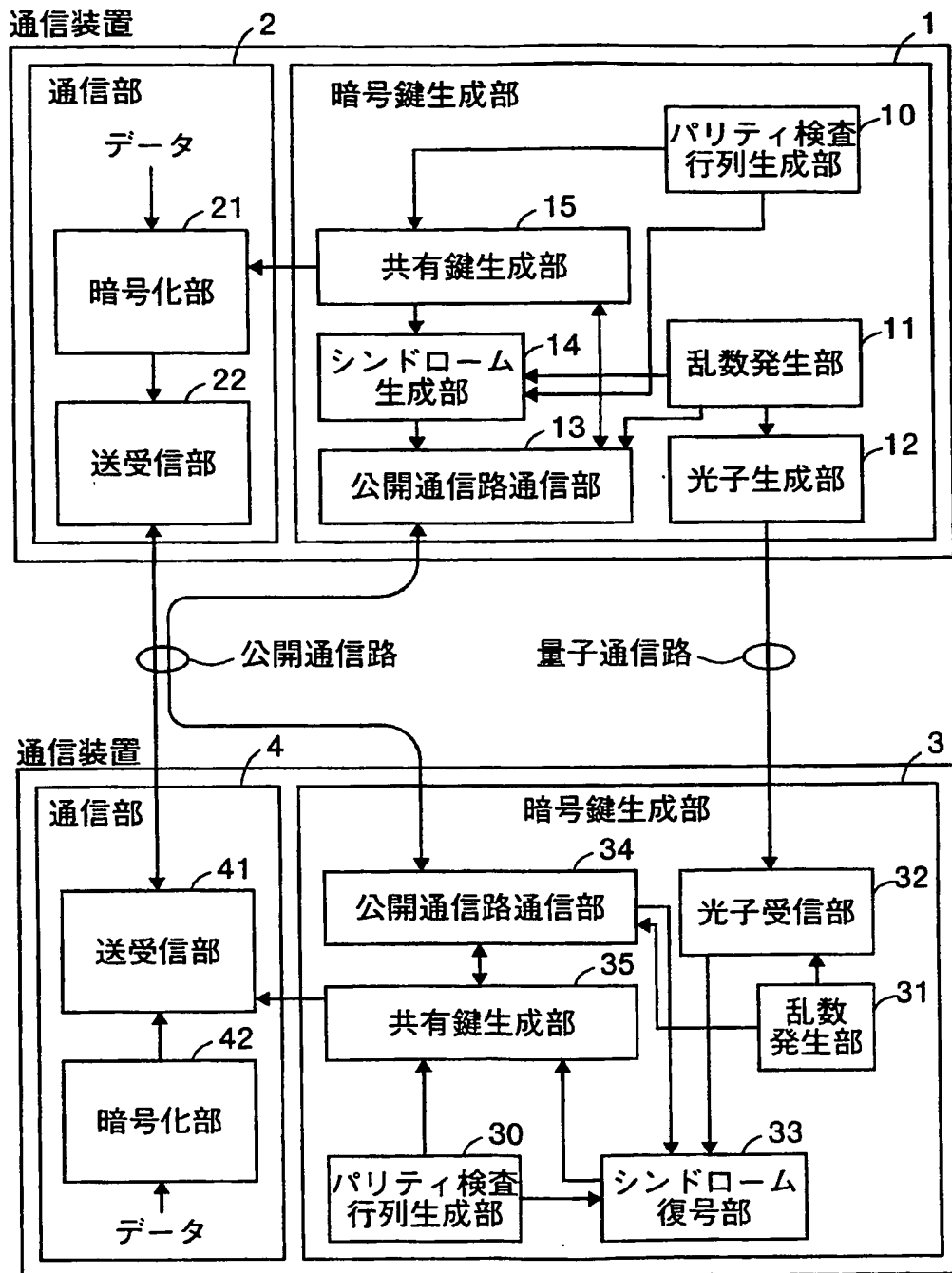
【符号の説明】

1, 1a, 3 暗号鍵生成部、2, 4 通信部、10, 30 パリティ検査行列生成部、11, 31 乱数発生部、12 光子生成部、13, 34 公開通路通信部、14 シンドローム生成部、15, 35 共有鍵生成部、21, 42 暗号化部、22, 41 送受信部、32 光子受信部、33 シンドローム復号部。

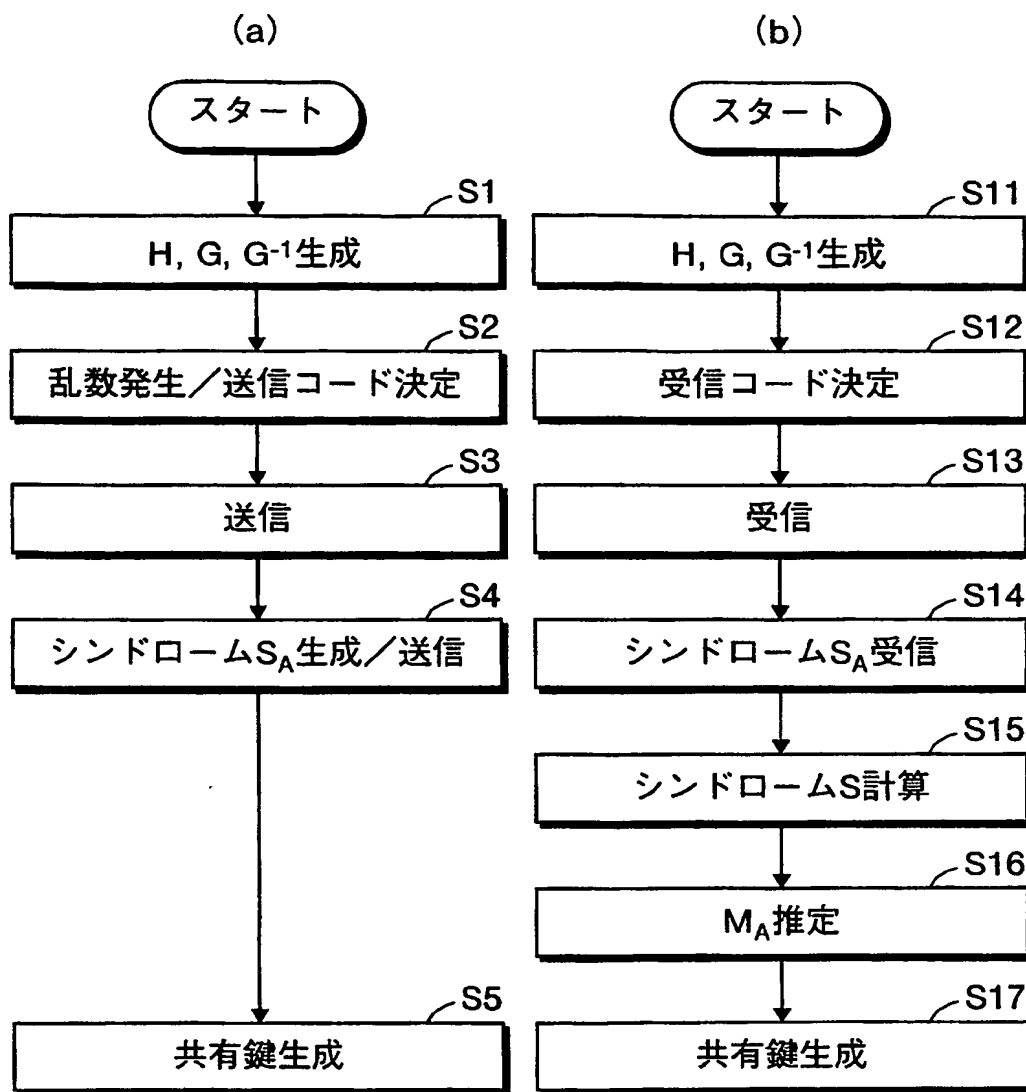
【書類名】

図面

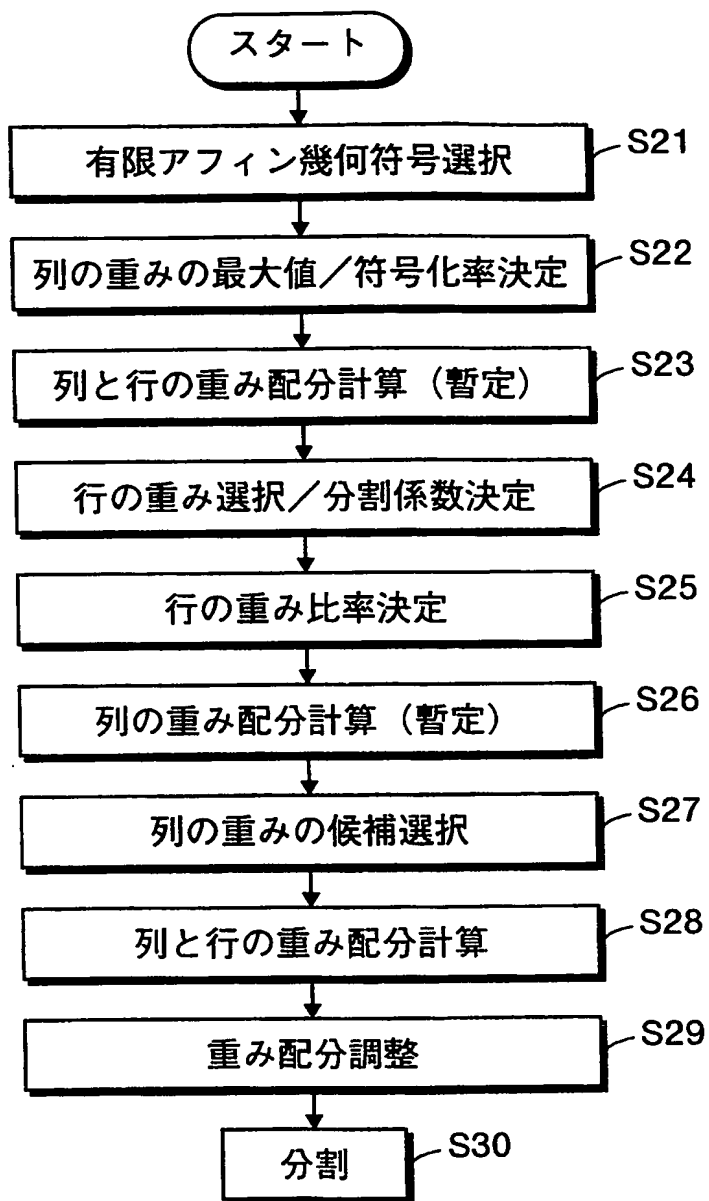
【図 1】



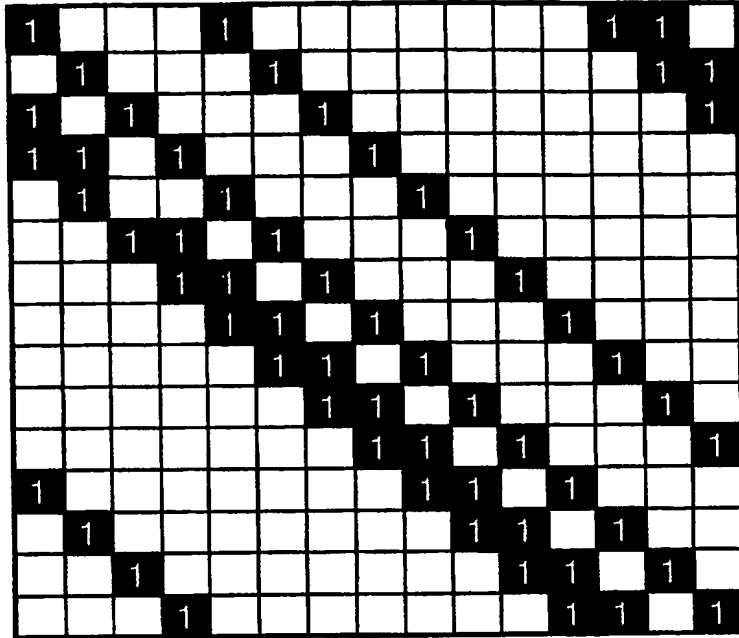
【図 2】



【図 3】



【図 4】

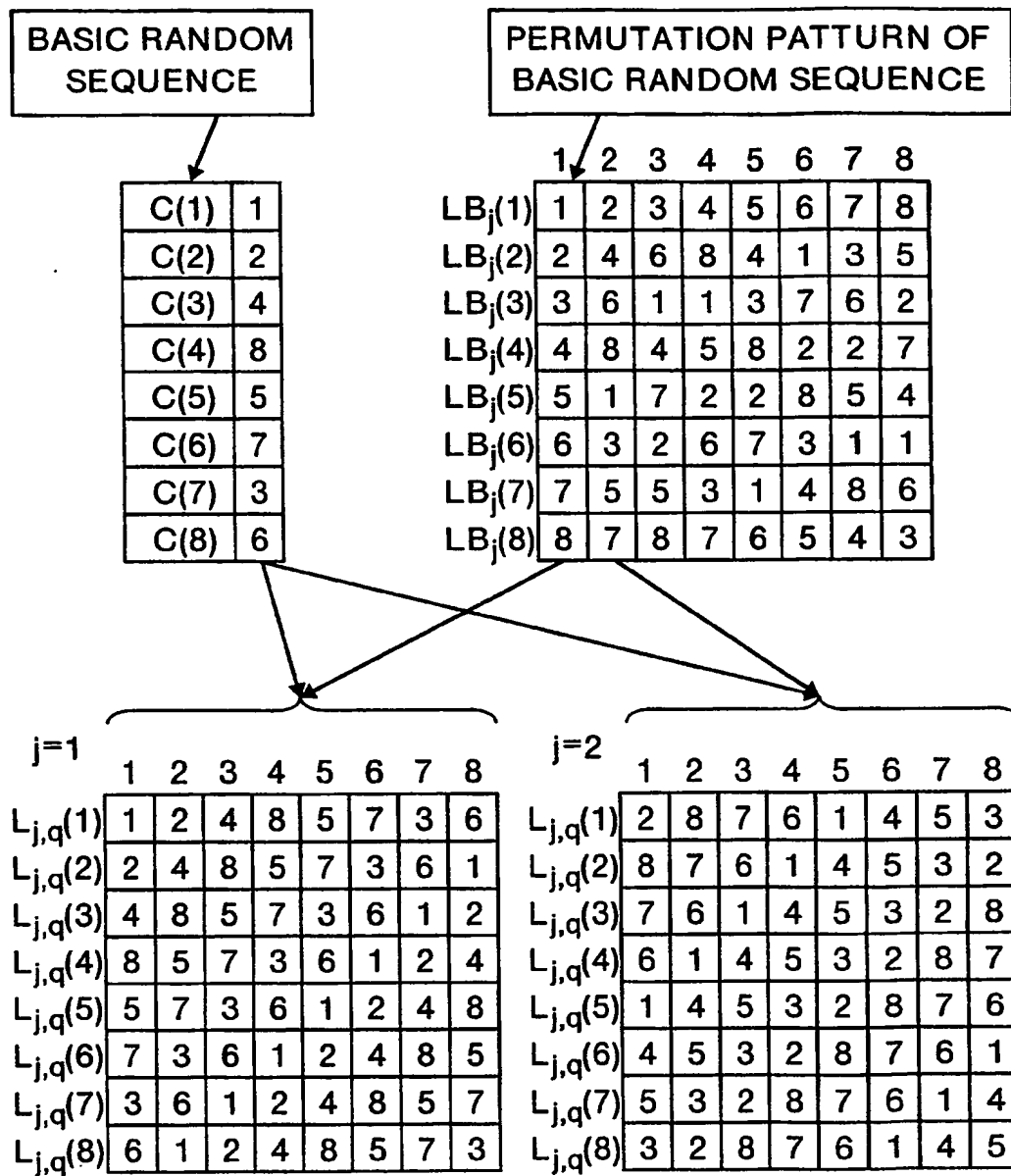


BEST AVAILABLE COPY

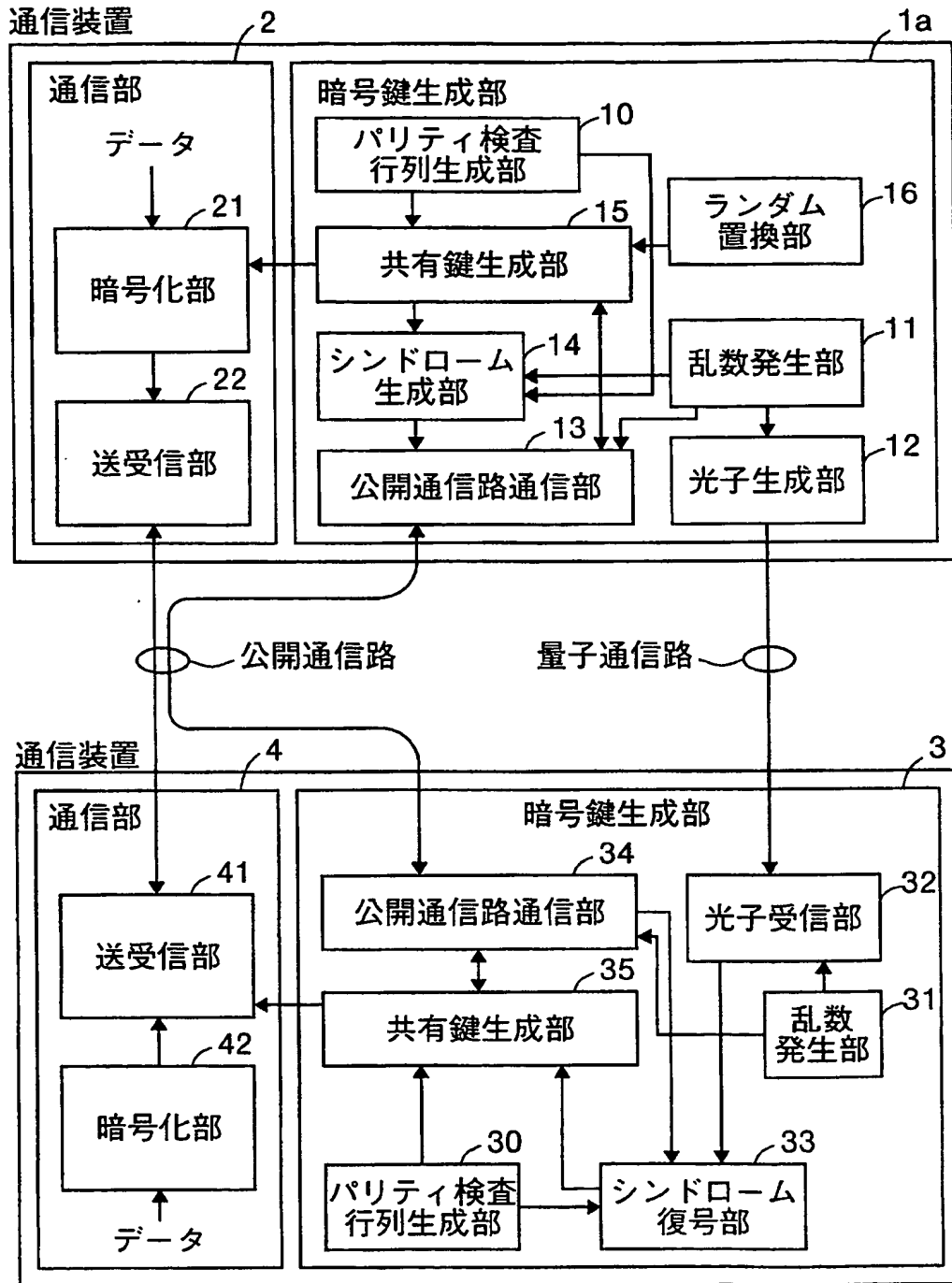
【図 5】

rate		0.5	
N		12.6	
i	γ_i	$\lambda(\gamma_i)$	$n(\gamma_i)$
1	2	0.27381	69
2	3	0.10714	18
3	8	0.61905	39
μ		ρ_μ	n_μ
8		1	63

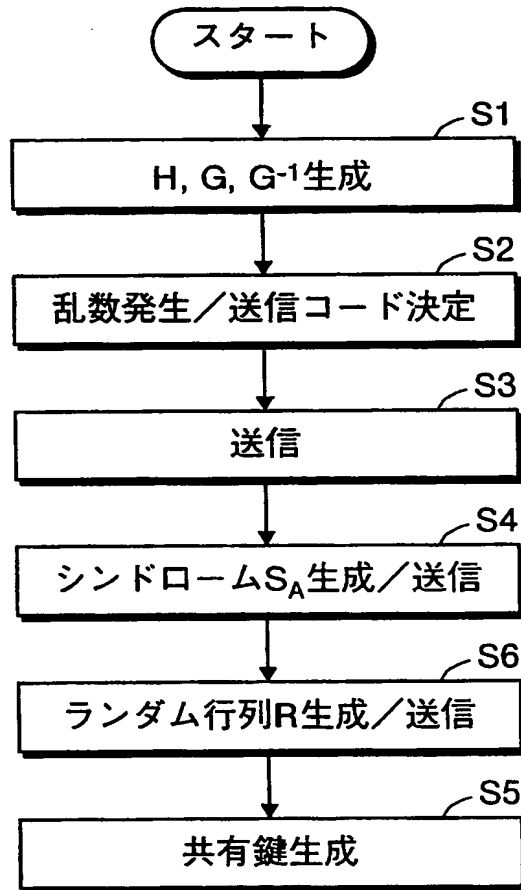
【図 6】



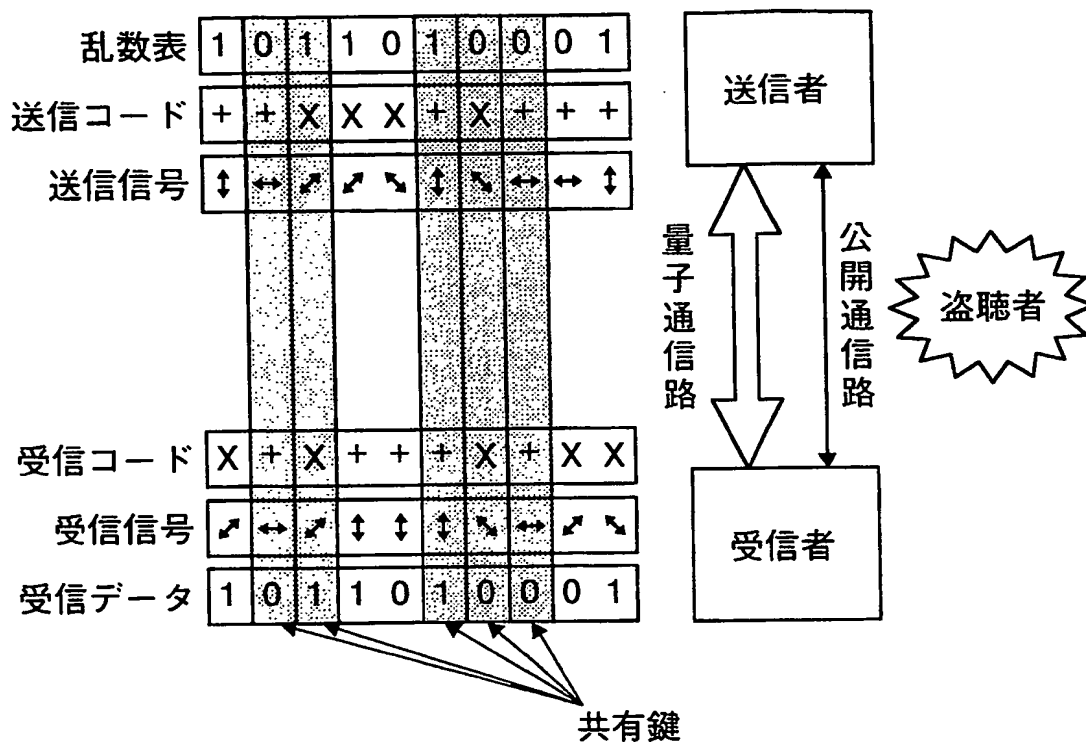
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法を得ること。

【解決手段】 本発明の量子鍵配送方法では、受信側の通信装置が、確定的で特性が安定した「Irregular-LDPC符号」用のパリティ検査行列を用いて受信データのデータ誤りを訂正し、受信側の通信装置および送信側の通信装置が、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。

【選択図】 図1

特願 2 0 0 2 - 2 7 1 4 7 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 0 1 3]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

東京都千代田区丸の内 2 丁目 2 番 3 号

氏 名

三菱電機株式会社

特願 2002-271473

出願人履歴情報

識別番号

[000006792]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

埼玉県和光市広沢2番1号

氏 名

理化学研究所